BTS SIO SISR 2 Godefroy de Bouillon

Mise en place d'un portail captif pfSense sur ESXi.

Dossier PPE

Barlet Pierre – Cheminade Julien – Mdere Faissoil

Sommaire

I. Introduction 3
II. Présentation du contexte 4
III. Liste des besoins 5
IV. Manuel Technique 6
A. Configuration ESXi 6
B. Configuration de pfSense 7
C. Configuration de la borne wifi 9
D. Configuration du serveur RADIUS 11
V. Diagramme de Gantt 13
VI. Manuel Utilisateur 14
VII. Références bibliographiques 14
VIII. Conclusion 15

I. Introduction

Tout d'abord nous allons présenter les notions qui seront abordé dans ce dossier.

PfSense : basé sur FreeBSD, c'est un routeur/pare-feu.
Portail captif : un portail captif force les clients HTTP d'un réseau de consultation à afficher une page web spéciale (le plus souvent dans un but d'authentification) avant d'accéder à Internet normalement.
RADIUS : Le protocole RADIUS (Remote Authentication Dial-In User Service) est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau.

II. Présentation du contexte

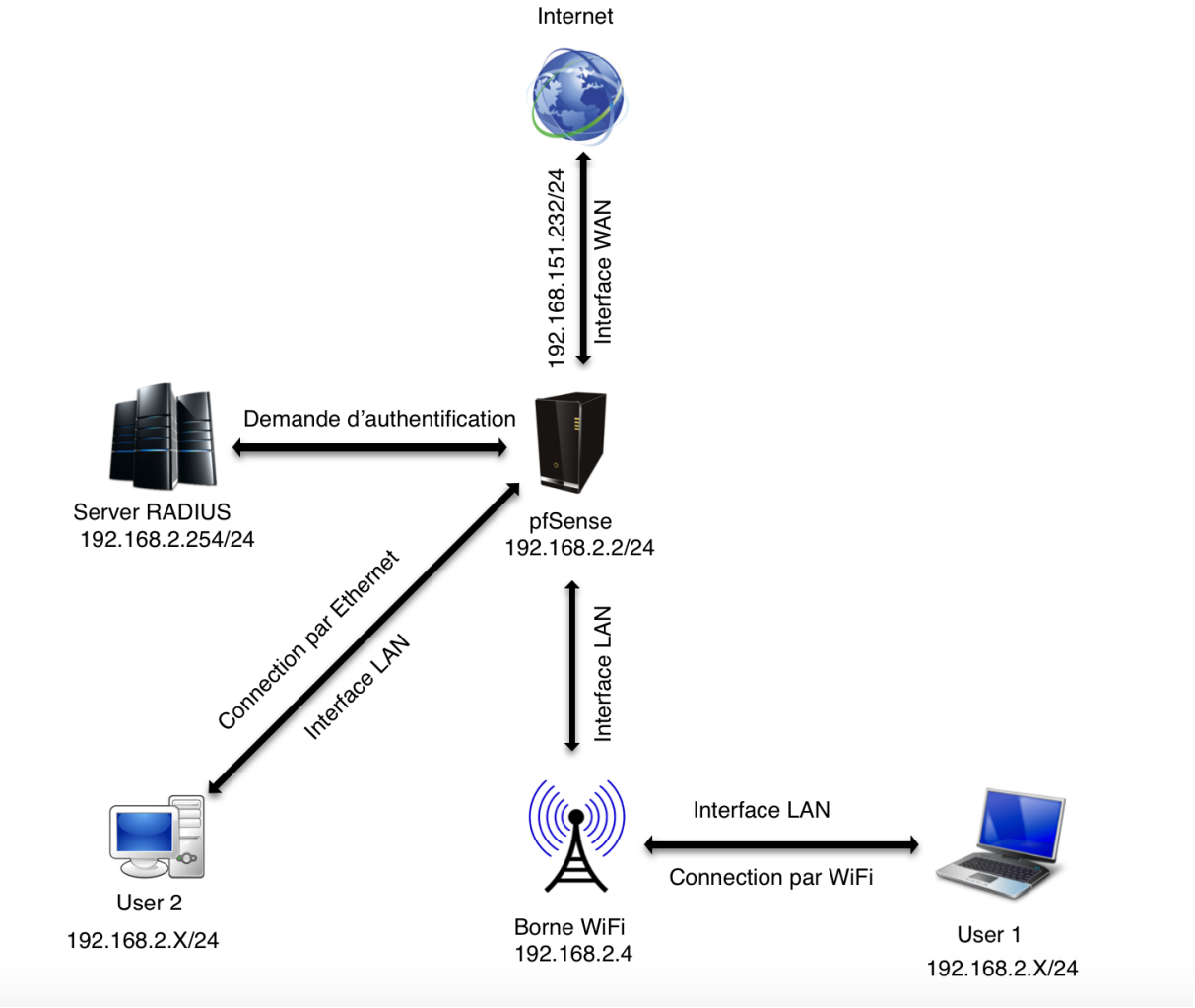
La société GSB à fait appel à notre équipe pour la mise en place d'une zone wifi sécurisé dans la salle de repos de leur siège. Afin de répondre le mieux aux attentes de la société, nous avons décidé de mettre en place un portail captif permettant aux utilisateurs appartenant au contrôleur de domaine de se connecter en utilisant leurs identifiants. Nous allons donc mettre en place un serveur de virtualisation ESXi pour installer pfSense ainsi qu'un serveur radius sur Windows 2008R2 qui authentifiera les utilisateurs. Pour des raisons matérielles nôtre projet à était fait entièrement en virtualisation.

III. Liste des besoins

Afin de réaliser correctement notre projet, nous avons dressé la liste suivante :

- 3 machines physiques
- Une borne Wifi
- Un serveur virtuel ESXi
- Une machine virtuelle pfSense
- Une machine virtuelle Windows Server 2008 R2 (contrôleur de domaine et serveur d'authentification RADIUS)
- Une ou plusieurs machines virtuelles Windows 7 clients

Architecture de notre réseau :



IV. Manuel Technique

A. Configuration ESXi

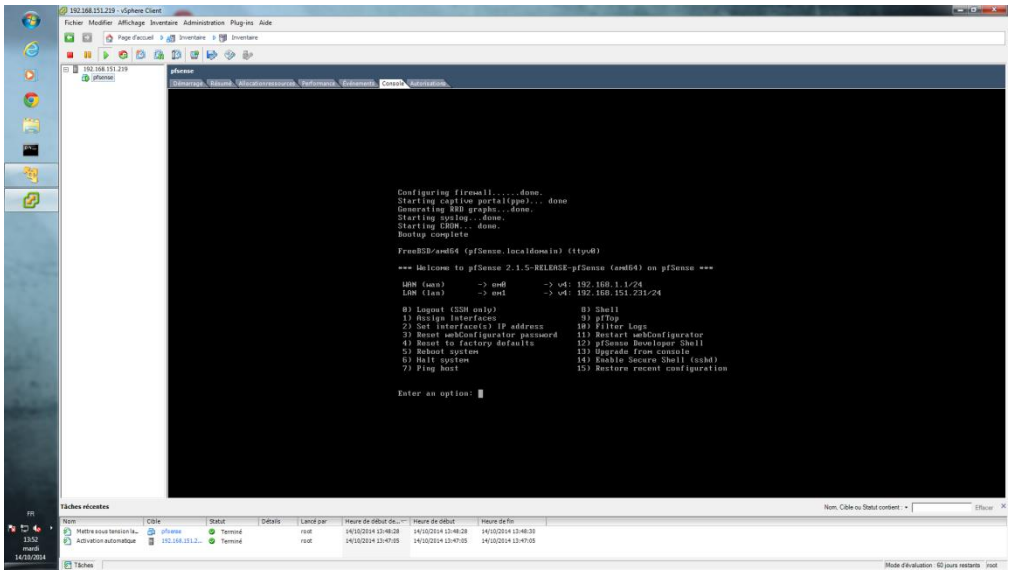
Tout d'abord nous avons installé une VM ESXi.

VMware ESXi 5.5.0 (VMKernel Release Build 1623387)
VMware, Inc. VMware Virtual Platform
2 x Intel(R) Core(TM) i3-3225 CPU @ 3.30GHz
4 GiB Memory
Download tools to manage this host from:
http://sio/
http://192.168.151.219/ (STATIC)
<F2> Customize System/View Logs
<F12> Shut Down/Restart

Puis nous avons mis en place pfSense sur ce serveur virtuel. Il s'agit donc d'un empilage de deux machines virtuelles.

B. Configuration de pfSense

Nous utilisons vSphere Client pour connecter et configurer la VM pfSense.

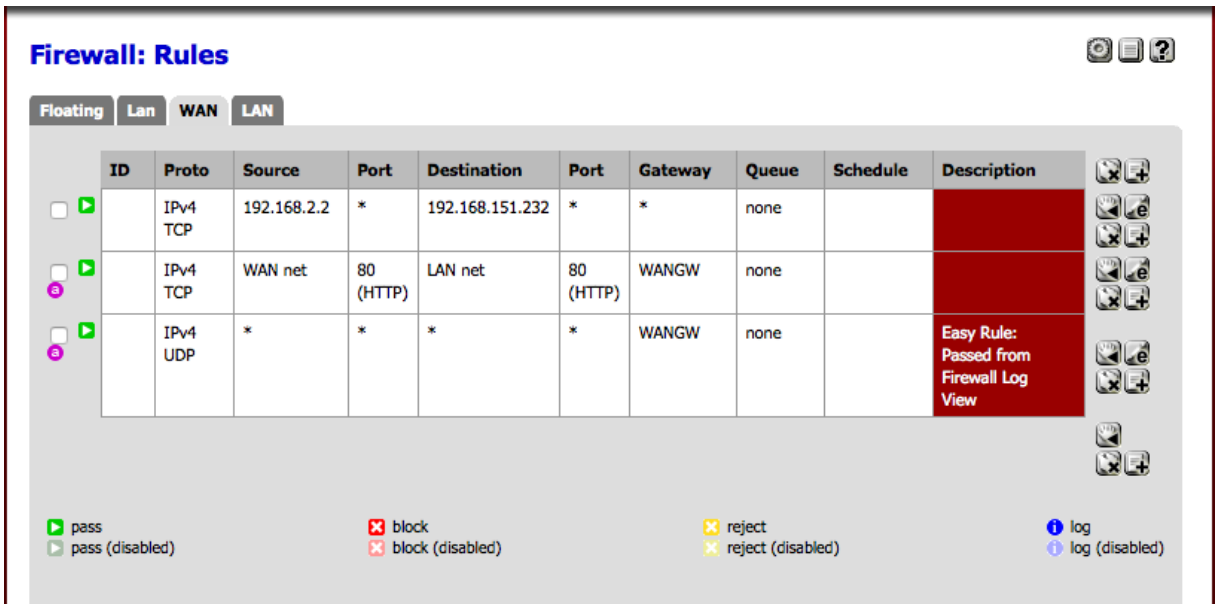


Nous avons défini 2 interfaces :

-WAN : 192.168.151.219

Nous avons mis cette adresse IP fixe du domaine sio.local pour accéder à internet via l'ESXi.

Les adresses après 200 n'étant pas attribuées par le DHCP, nous avons choisi arbitrairement l'adresse 219.



-LAN : 192.168.2.2

Cette adresse ip correspond au réseau où les machines clients se trouvent.

L'accès à la configuration du pfSense se fait via le navigateur.

Firewall: Rules

Floating | Lan | WAN | LAN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓		*	*	*	LAN Address	80 22	*	*		Anti-Lockout Rule
✓		IPv4 TCP	192.168.151.232	*	192.168.2.2	*	*	none		
✓		IPv4 TCP	WAN net	*	LAN net	*	WANGW	none		
✓		IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
✓		IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule

pass / pass (disabled) — block / block (disabled) — reject / reject (disabled) — log / log (disabled)

System: General Setup

System

Hostname: pf
Name of the firewall host, without domain part
e.g. *firewall*

Domain: pfsense.local
Do not use 'local' as a domain name. It will cause local hosts running mDNS (avahi, bonjour, etc.) to be unable to resolve local hosts not running mDNS.
e.g. *mycorp.com, home, office, private, etc.*

DNS servers

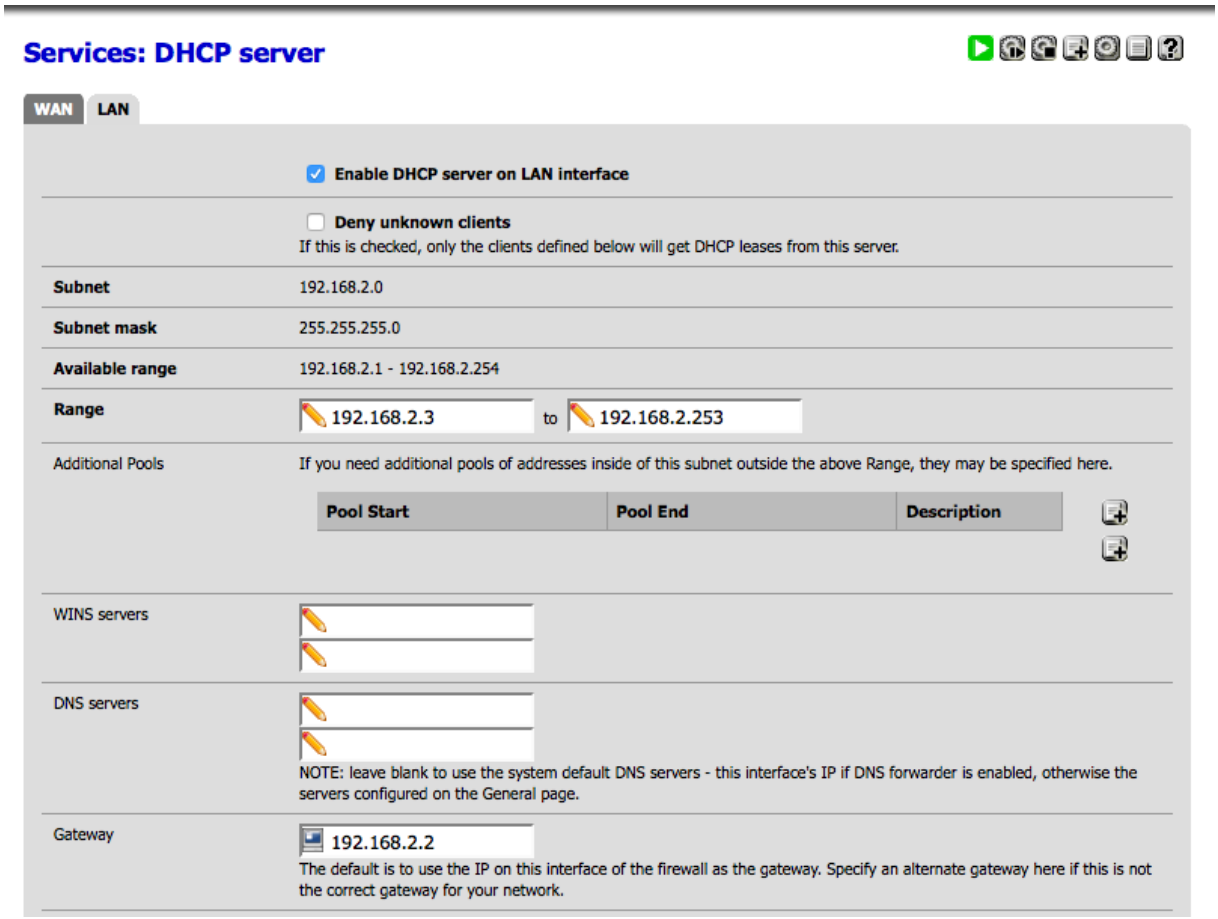
DNS Server	Use gateway
192.168.151.254	WANGW - wan - 192.168.151.254
	none
	none
	none

Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS forwarder and for PPTP VPN clients.

In addition, optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.

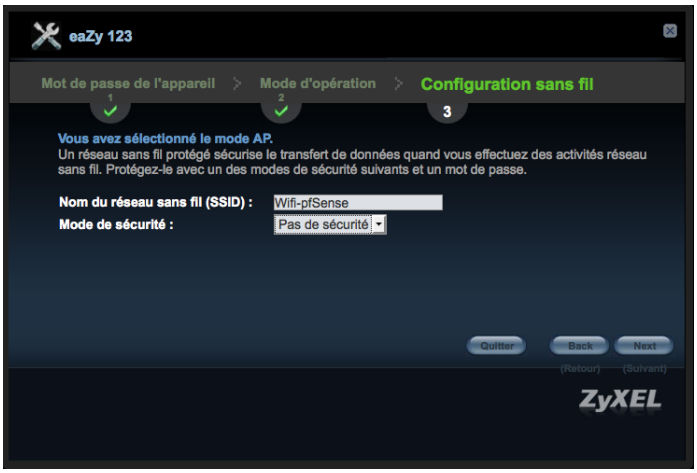
☑ **Allow DNS server list to be overridden by DHCP/PPP on WAN**
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). However, they will not be assigned to DHCP and PPTP VPN clients.

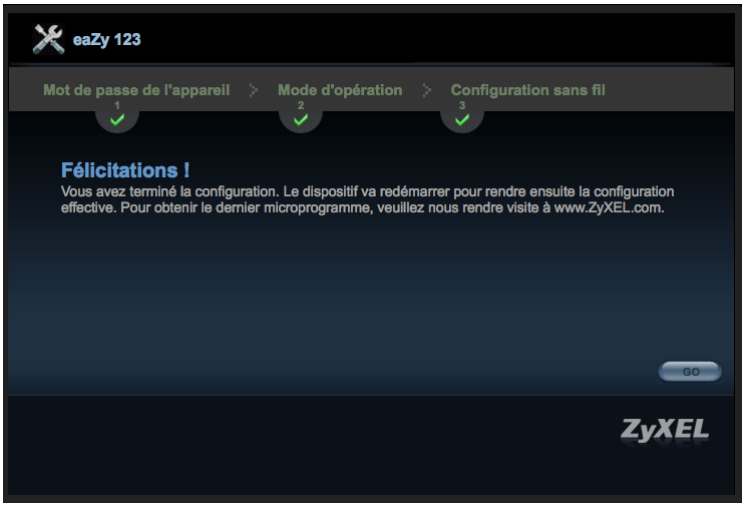
DHCP de l'interface LAN :


Services: DHCP server
WAN
LAN
Enable DHCP server on LAN interface
Deny unknown clients
If this is checked, only the clients defined below will get DHCP leases from this server.
Subnet
192.168.2.0
Subnet mask
255.255.255.0
Available range
192.168.2.1 - 192.168.2.254
Range
192.168.2.3
to
192.168.2.253
Additional Pools
If you need additional pools of addresses inside of this subnet outside the above Range, they may be specified here.
Pool Start
Pool End
Description
WINS servers
DNS servers
NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS forwarder is enabled, otherwise the servers configured on the General page.
Gateway
192.168.2.2
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network.

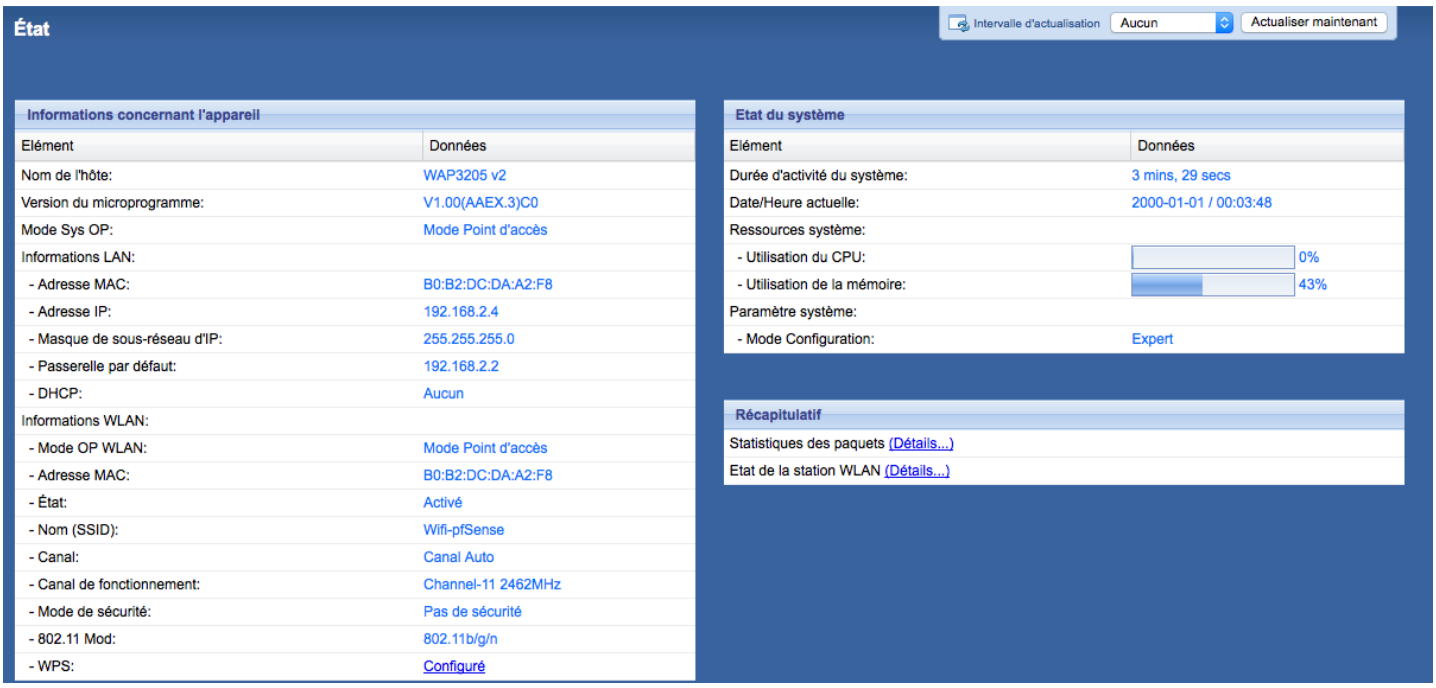
C. Configuration de la borne wifi

eaZy 123
Mot de passe de l'appareil
Mode d'opération
Configuration sans fil
Mode Configuration
Sélectionnez le mode Répéteur universel pour vous connecter à un WLAN spécifique et pour que l'appareil agisse en même temps comme un AP. Sélectionnez le mode Point d'accès pour utiliser l'appareil comme un point d'accès standard. Sélectionnez le mode Client si vous souhaitez utiliser cet appareil comme une carte réseau sans fil.
The current operation mode is: Mode Point d'accès
Quitter
Back
Next
ZyXEL


eaZy 123
Mot de passe de l'appareil
Mode d'opération
Configuration sans fil
1
2
3
Vous avez sélectionné le mode AP.
Un réseau sans fil protégé sécurise le transfert de données quand vous effectuez des activités réseau sans fil. Protégez-le avec un des modes de sécurité suivants et un mot de passe.
Nom du réseau sans fil (SSID) :
Wifi-pfSense
Mode de sécurité :
Pas de sécurité
Quitter
Back
(Retour)
Next
(Suivant)
ZyXEL


eaZy 123
Mot de passe de l'appareil
Mode d'opération
Configuration sans fil
1
2
3
Félicitations !
Vous avez terminé la configuration. Le dispositif va redémarrer pour rendre ensuite la configuration effective. Pour obtenir le dernier microprogramme, veuillez nous rendre visite à www.ZyXEL.com.
GO
ZyXEL

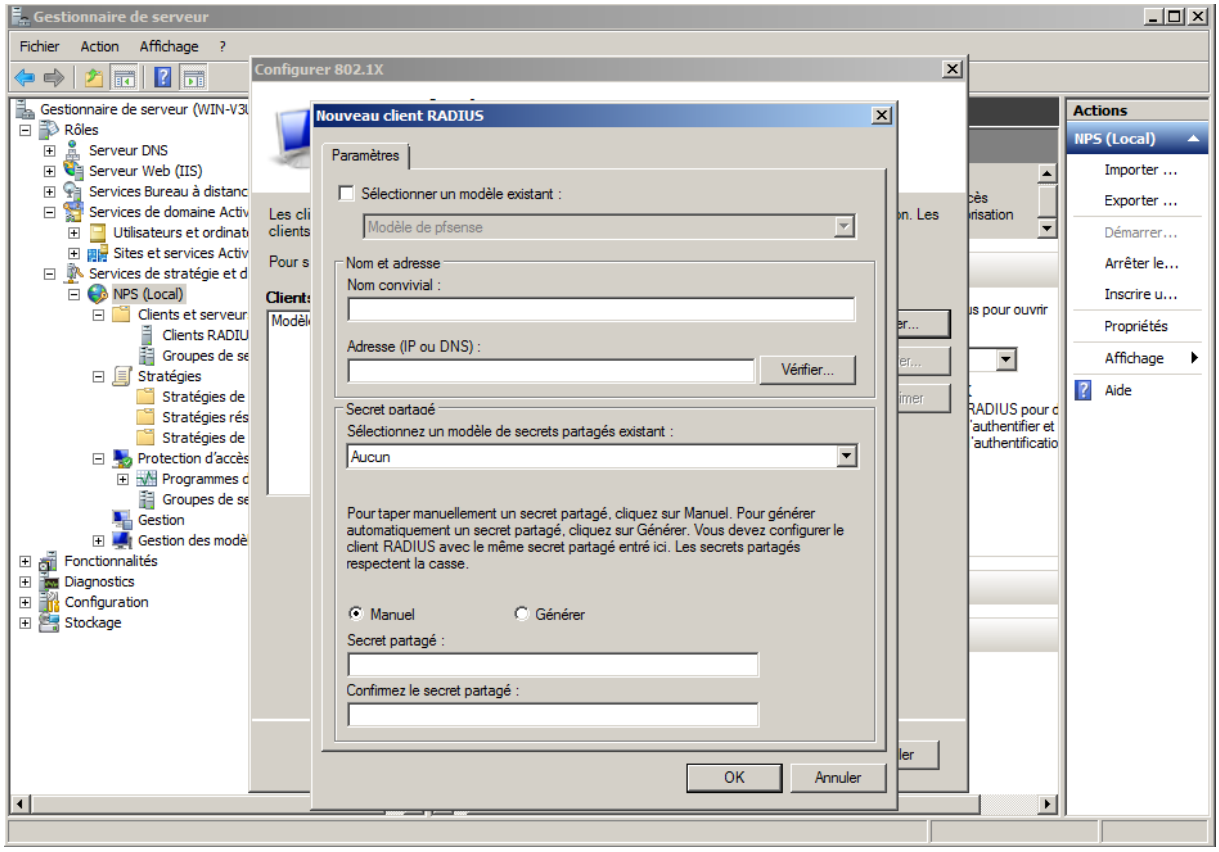
eaZy 123
Mot de passe de l'appareil
Mode d'opération
Configuration sans fil
1
2
3
Appareil va redémarrer maintenant.
L'appareil redémarrera maintenant. Veuillez attendre une minute avant de tenter d'accéder de nouveau au périphérique.
Chargement...
ZyXEL

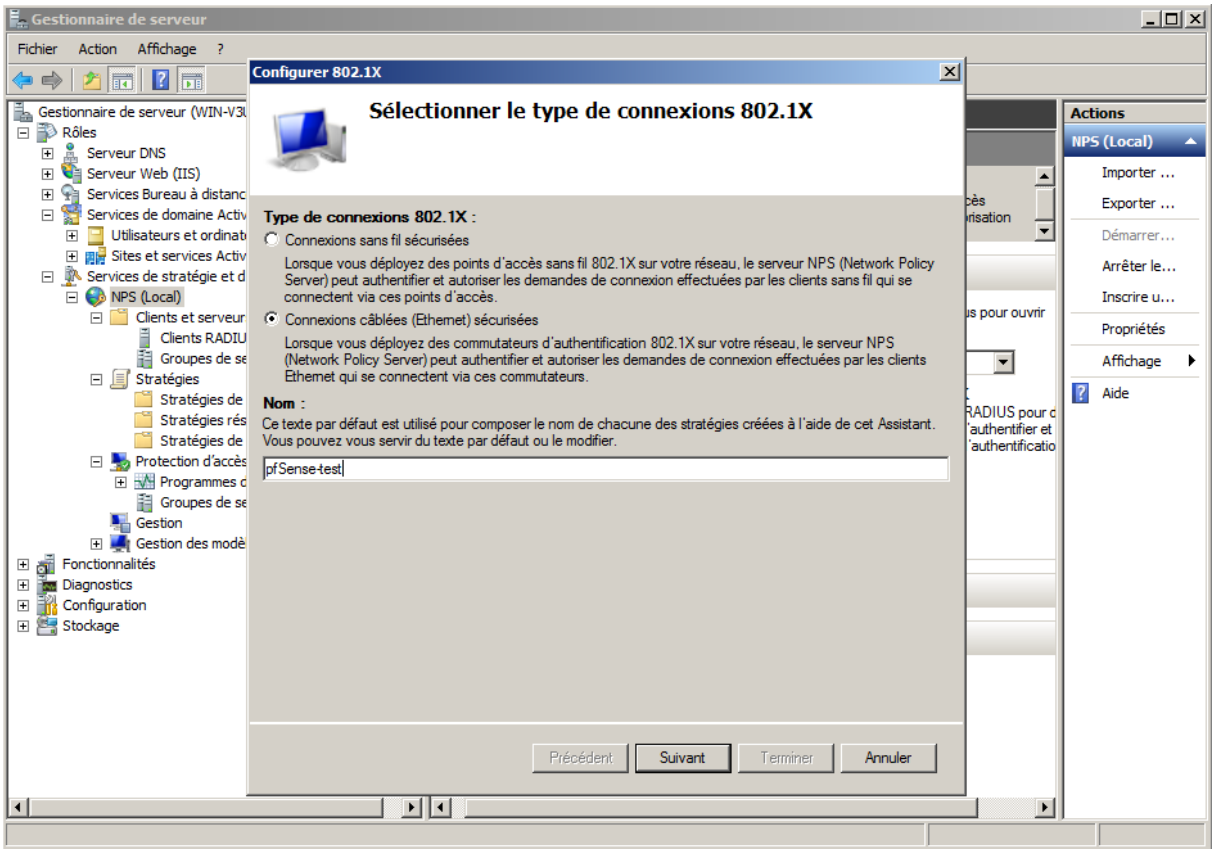

État
Intervalle d'actualisation
Aucun
Actualiser maintenant
Informations concernant l'appareil
Elément
Données
Nom de l'hôte: WAP3205 v2
Version du microprogramme: V1.00(AAEX.3)C0
Mode Sys OP: Mode Point d'accès
Informations LAN:
- Adresse MAC: B0:B2:DC:DA:A2:F8
- Adresse IP: 192.168.2.4
- Masque de sous-réseau d'IP: 255.255.255.0
- Passerelle par défaut: 192.168.2.2
- DHCP: Aucun
Informations WLAN:
- Mode OP WLAN: Mode Point d'accès
- Adresse MAC: B0:B2:DC:DA:A2:F8
- État: Activé
- Nom (SSID): Wifi-pfSense
- Canal: Canal Auto
- Canal de fonctionnement: Channel-11 2462MHz
- Mode de sécurité: Pas de sécurité
- 802.11 Mod: 802.11b/g/n
- WPS: Configuré
Etat du système
Elément
Données
Durée d'activité du système: 3 mins, 29 secs
Date/Heure actuelle: 2000-01-01 / 00:03:48
Ressources système:
- Utilisation du CPU: 0%
- Utilisation de la mémoire: 43%
Paramètre système:
- Mode Configuration: Expert
Récapitulatif
Statistiques des paquets (Détails...)
Etat de la station WLAN (Détails...)

D. Configuration du serveur RADIUS

Avant tout ajouté la fonctionnalité NPS (Network Policy Server) en suite créer une stratégie qui permet au server NPS d'authentifier et d'autoriser les connexions.

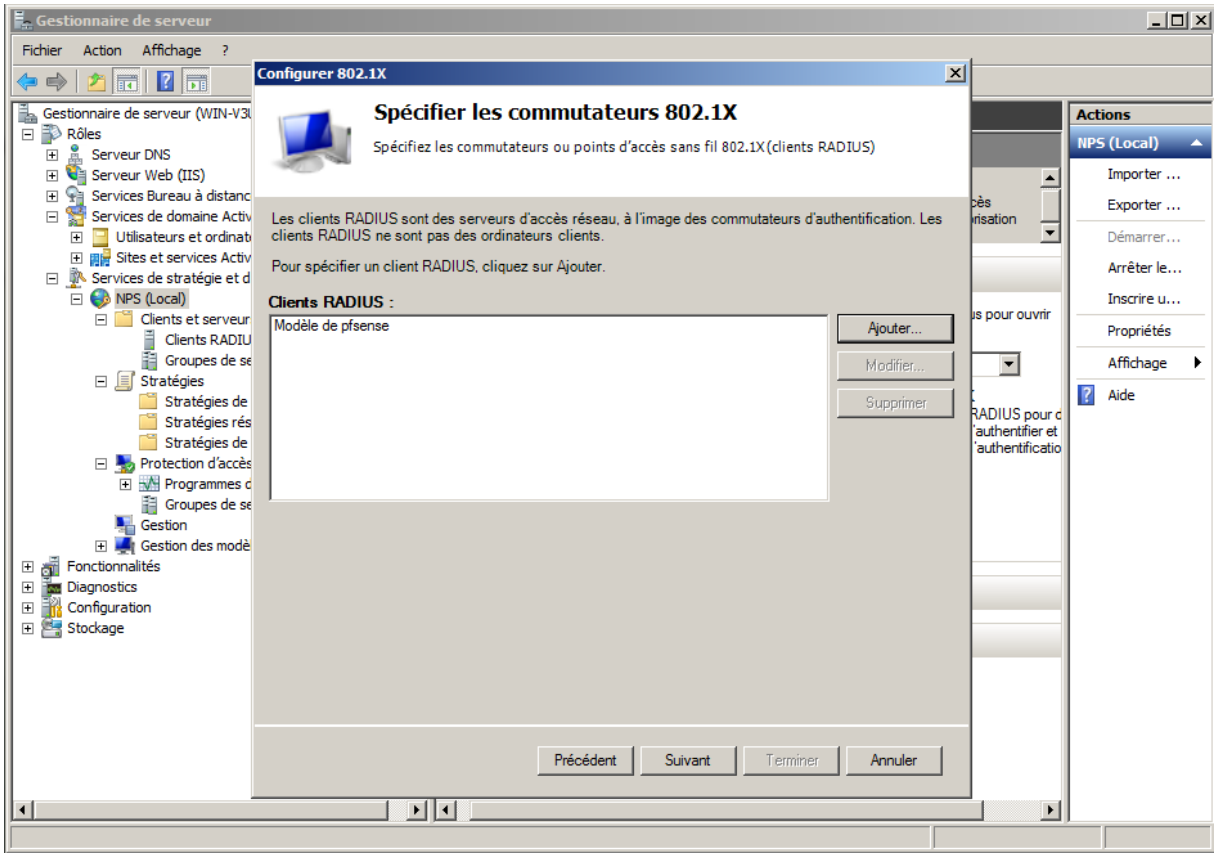
Sélectionner le type de connexion Ethernet ou sans fil




Gestionnaire de serveur
Fichier Action Affichage ?
Configurer 802.1X
Sélectionner le type de connexions 802.1X
Type de connexions 802.1X :
Connexions sans fil sécurisées
Lorsque vous déployez des points d'accès sans fil 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients sans fil qui se connectent via ces points d'accès.
Connexions câblées (Ethernet) sécurisées
Lorsque vous déployez des commutateurs d'authentification 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients Ethernet qui se connectent via ces commutateurs.
Nom :
Ce texte par défaut est utilisé pour composer le nom de chacune des stratégies créées à l'aide de cet Assistant. Vous pouvez vous servir du texte par défaut ou le modifier.
pfSense-test
Précédent
Suivant
Terminer
Annuler
Actions
NPS (Local)
Importer ...
Exporter ...
Démarrer...
Arrêter le...
Inscrire u...
Propriétés
Affichage
Aide

Ajouter un nouveau client Radius

Configurer adresse IP ou DNS et ne pas oublier le secret partagé.

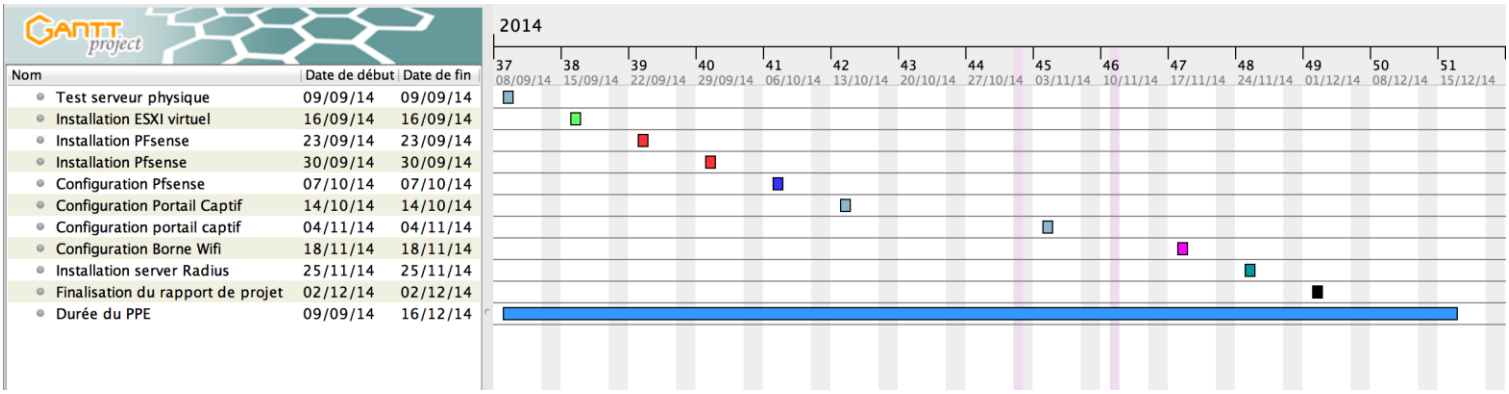


NPS

Le serveur NPS vous permet de créer et de mettre en application sur l'ensemble du réseau de votre organisation des stratégies d'accès réseau portant sur l'intégralité des clients, ainsi que sur l'authentification et l'autorisation des demandes de connexion.

Attention sur le Windows serveur 2003 c'est IAS (internet authentification service)

V. Diagramme de Gantt



VI. Manuel Utilisateur

Voir annexe fourni avec le dossier.

VII. Références bibliographiques

Pour nous aider dans la configuration des différents éléments qui constituent notre projet nous avons utilisé plusieurs documents :

- INSTALLATION D'UN PORTAIL CAPTIF PERSONNALISE PFSENSE par Aurélien JAULENT
- pfSense *Manuel d'Installation et d'Utilisation du Logiciel* par Yannick LAGARDE
- Mise en œuvre d'un Portail Captif sur un réseau WIFI par Anthony LYLIAN
- Nous avons aussi consulté le forum pfSense

VIII. Conclusion

Pour mener à bien notre projet, nous voulions installer un ESXi sur une machine physique, mais il nous a était impossible de réaliser cette installation pour des raisons matérielles (problèmes de versions ESXi/architecture processeur supportée). Nous avons donc choisi de nous servir de VMWarePlayer pour l'ESXi. La virtualisation nous donne plus de liberté mais nous avons rencontré de nombreux problèmes de réseaux, conflit d'adresses IP principalement.
Vers la fin du PPE nous avons aussi rencontré des problèmes de latence avec l'une des bornes Wifi.